UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/836,952	04/17/2001	Mehrban Jam	10005248-1	6956

7590 06/18/2008

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
EHICHIOYA, FRED I	
ART UNIT	PAPER NUMBER
2162	
MAIL DATE	DELIVERY MODE
06/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/836,952
Filing Date: April 17, 2001
Appellant(s): JAM, MEHRBAN

Dan C. Hu, Reg. No. 40,025
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed March 12, 2008 appealing from the Office action mailed November 15, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

NEW GROUND(S) OF REJECTION

Claims 13 – 19 and 31 – 35 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Ljungh Robert et al., "WIPS Technical Documentation", Royal Institute of Technology, (May 25, 2000), pages 1 - 19.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

NEW GROUND(S) OF REJECTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 13 – 19 and 31 - 35 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 13 and 31 are directed to a computer-usable medium embodying computer code. Though computer-usable medium is disclosed on page 2 of the specification (see amendment to specification of September 4, 2007); this medium is neither defined by the specification nor drawings as a physical object; one of ordinary skills in the art at the time of present invention will not consider applicant's claimed computer-usable medium to be a physical device that constitutes a machine within the meaning of 101 and therefore non-statutory (MPEP 2106.01 [R-5] (I)).

Regarding claims 14 – 19 and 32 - 35, these claims depend from claims 13 and 31 respectively, recite computing steps, are merely descriptive and lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101 and therefore non-statutory.

Claim Rejections - 35 USC § 102

Claims 1 – 38 are rejected under 35 U.S.C. 102(e) as being anticipated by Non-Patent Literature (NPL) "WIPS Technical Documentation by Roland Ljungh et al., (Hereinafter "Ljungh").

Regarding claim 1, Ljungh disclose a computer-implemented method comprising:

assigning information stored on a computer a plurality of clearance levels (see page 13, section 4.1.2, paragraph 1 wherein "access levels" is interpreted as "clearance levels" and the administrator assigns or determines who is able to view which information);

assigning each smart badge within a set of smart badges one of the clearance levels (see page 15, section 4.2.1 wherein the doors are assigned security levels. The badge is associated with the door for authorizing access; inherently, badges are assigned access or clearance level in other to have a particular entry through these doors);

using a wireless beacon to detect which smart badges are located within a predefined boundary (see page 1, section 1, paragraph 2 wherein badges and location of the badges are identified using the IR beacons);

identifying a lowest clearance level assigned to the smart badges within the boundary (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level (see page 15, section 4.2.1 discusses providing different security levels to different doors within a building. Different security levels are sub-set of the whole security system. On page 6, Ljungh discloses information about which badge a person is wearing and the IP address of his laptop. The badge is assumed to have static IP addresses. Further on page 7, Ljungh discloses “the database server has a method of finding out whether or not a particular user is allowed to see and update certain information in the database. These pages and section clearly suggests applicants claimed limitation “providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level").

Regarding claims 2 and 14, Ljungh discloses defining those smart badges within the boundary as a set of visible smart badges (see page 1, section 1, paragraph 2 wherein a person wearing WIPS badge is interpreted as visible smart badge); and

updating the set of visible smart badges in response to a change in smart badge visibility status (see page 1, section 1, paragraph 2 wherein the badge server is updated when the person wearing the WIPS badge moves from one place to the other).

Regarding claims 3 and 15, Ljungh discloses recalculating the lowest clearance level in response to the change in smart badge visibility status (see page 5, paragraph 1 wherein person events is generated when moved from one room to another in the re-access the security access level).

Regarding claim 4, Ljungh discloses the method of claim 2 further comprising:

recording the smart badge visibility status of each smart badge within an activity log (see page 10, section 3.3.1, paragraph 1 wherein the show room enables writing the name of specific room, badge/person wearing the badge when there is movement activities).

Regarding claims 5 and 16, Ljungh discloses providing access to smart badge wearers assigned to the smart badges (see page 15, section 4.2.1 wherein access is granted to badge wearer).

Regarding claims 6 and 17, Ljungh discloses the method of claim 2 further comprising:

preventing access to the information when the smart badge visibility status is set to invisible for a predetermined timeout (see page 9, paragraph 1 wherein access is denied when connection with the badge closes or timeout occurs).

Regarding claim 7, Ljungh discloses the method of claim 1 further comprising: writing data items to the smart badges (see page 9, paragraph 6 wherein commands are used to configure/ or write on the badge).

Regarding claim 8, Ljungh discloses the method of claim 7 further comprising:

pre-reading the data items from the smart badges during idle periods (see page 9, paragraph 5 wherein data is red from the badge).

Regarding claims 9 and 18, Ljungh discloses defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers (see page 15, section 4.2.1 paragraph 1 wherein the badge is authenticated to verify that the badge is in the possession of the owner).

Regarding claims 10 and 19, Ljungh discloses assigning an expiration period to each of the smart badges (see page 9, paragraph 1 wherein the timeouts is interpreted as the expiration time); and

de-authenticating and erasing all data stored on a smart badge whose expiration period has been exceeded (see page 14, section 4.1.5 paragraph 2 wherein the administrator can edit or remove data from the badge).

Regarding claim 11, Ljungh discloses the method of claim 1 wherein the using element includes:

configuring the predefined boundary by varying a sensitivity level of the wireless beacon (see page 15, paragraph 1 wherein beacons are created according to the sensitivity level for example – light or dark sensitivity).

Regarding claim 12, Ljungh discloses a method for context-aware computer management comprising:

assigning database information a plurality of clearance levels (see page 13, section 4.1.2, paragraph 1 wherein “access levels” is interpreted as “clearance levels” and the administrator assigns or determines who is able to view which information);

assigning each smart badge within a set of smart badges one of the clearance levels (see page 15, section 4.2.1 wherein the doors are assigned security levels. The badge is associated with the door for authorizing access; inherently, badges are assigned access or clearance level in other to have a particular entry through these doors);

using a wireless beacon to detect which smart badges are located within a predefined boundary (see page 1, section 1, paragraph 2 wherein badges and location of the badges are identified using the IR beacons);

identifying a lowest clearance level assigned to the smart badges within the boundary (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access);

defining those smart badges within the boundary as a set of visible smart badges (see page 1, section 1, paragraph 2 wherein a person wearing WIPS badge is interpreted as visible smart badge);

updating the set of visible smart badges in response to a change in smart badge visibility status (see page 1, section 1, paragraph 2 wherein the badge server is updated when the person wearing the WIPS badge moves from one place to the other); and recalculating the lowest clearance level in response to the change in smart badge visibility status (see page 5, paragraph 1 wherein person events is generated when moved from one room to another in the re-access the security access level).

Regarding claim 13, Ljungh discloses a computer-usable medium embodying computer program code for context-aware computer management, comprising:

assigning database information a plurality of clearance levels (see page 13, section 4.1.2, paragraph 1 wherein “access levels” is interpreted as “clearance levels” and the administrator assigns or determines who is able to view which information);

assigning each smart badge within a set of smart badges one of the clearance levels (see page 15, section 4.2.1 wherein the doors are assigned security levels. The badge is associated with the door for authorizing access; inherently, badges are assigned access or clearance level in other to have a particular entry through these doors);

using a wireless beacon to detect which smart badges are located within a predefined boundary (see page 1, section 1, paragraph 2 wherein badges and location of the badges are identified using the IR beacons);

identifying a lowest clearance level assigned to the smart badges within the boundary (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 20, Ljungh discloses a system for context-aware computer management comprising:

means for assigning database information a plurality of clearance levels(see page 13, section 4.1.2, paragraph 1 wherein “access levels” is interpreted as “clearance levels” and the administrator assigns or determines who is able to view which information);

means for assigning each smart badge within a set of smart badges one of the clearance levels (see page 15, section 4.2.1 wherein the doors are assigned security levels. The badge is associated with the door for authorizing access; inherently, badges are assigned access or clearance level in other to have a particular entry through these doors);

means for using a wireless beacon to detect which smart badges are located within a predefined boundary (see page 1, section 1, paragraph 2 wherein badges and location of the badges are identified using the IR beacons);

means for identifying a lowest clearance level assigned to the smart badges within the boundary (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

means for providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access);

means for defining those smart badges within the boundary as a set of visible smart badges (see page 1, section 1, paragraph 2 wherein a person wearing WIPS badge is interpreted as visible smart badge);

means for updating the set of visible smart badges in response to a change in smart badge visibility status (see page 1, section 1, paragraph 2 wherein the badge server is updated when the person wearing the WIPS badge moves from one place to the other); and

means for recalculating the lowest clearance level in response to the change in smart badge visibility status (see page 5, paragraph 1 wherein person events is generated when moved from one room to another in the re-access the security access level).

Regarding claim 21, Ljungh discloses a system for context-aware computer management comprising:

a database (see page 5, section 3.2.2), including information differentiated by a plurality of clearance levels (see page 13, section 4.1.2 wherein different access levels are disclosed);

a first wireless beacon (see page 1, section 1 paragraph 2 wherein the rooms are equipped with beacons which inherently include first and second beacons);

a set of smart badges, detected by the first wireless beacon to be within a predefined boundary (see page 1, section 1 paragraph 2 wherein the badge receives transmission from the beacon), each badge assigned one of the clearance levels (see page 13, section 4.1.2, paragraph 1 wherein “access levels” is interpreted as “clearance levels”);

computer located within the boundary (see page 16, section 4.2.5 wherein a portable computer is disclosed);

a system service module, coupled to the first wireless beacon (see Fig.1 wherein the beacon is connected to the badge/service module), for identifying a lowest clearance level assigned to the smart badges within the boundary (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

a software application, coupled to the system service module and the database, for providing access to that sub-set of the information within the database having a clearance level no higher than the lowest identified clearance level on the computer (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 22, Ljungh discloses the system of claim 21, wherein the first beacon includes: a wide angle RF beacon (see page 17, section A.2 wherein RF signal is placed as beacon).

Regarding claim 23, Ljungh discloses the system of claim 21, further comprising:

a second diffuse IR beacon, coupled to the service module, limited to detecting smart badges within the predefined boundary (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge).

Regarding claim 24, Ljungh discloses the system of claim 21, wherein the smart badges include:

biometric sensors for detecting when a smart badge has been removed from an assigned smart badge wearer (see page 15, section 4.2.1 wherein voice sensor is the biometric sensor).

Regarding claim 25, Ljungh discloses the system of claim 21, wherein the service module defines those smart badges within the boundary as a set of visible smart badges (see page 1, section 1, paragraph 2 wherein a person wearing WIPS badge is interpreted as visible smart badge), and

recalculates the lowest clearance level in response to a change in a visibility status (see page 5, paragraph 1 wherein person events is generated when moved from one room to another in the re-access the security access level).

Regarding claim 26, Ljungh discloses the system of claim 21, wherein the application logs smart badge wearers assigned to visible smart badges onto the computer (see page 10, section 3.3.1, paragraph 1 wherein the show room enables writing the name of specific room, badge/person wearing the badge when there is movement activities).

Regarding claim 27, Ljungh discloses the method of claim 1, wherein providing access to the sub-set of information comprises providing access to the sub-set of information stored on the computer located within the predefined boundary (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 28, Ljungh discloses the method of claim 1, wherein the wireless beacon comprises a first wireless beacon to communicate with the smart badges, the method further comprising:

using a second wireless beacon to communicate with the smart badges (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge),

wherein detecting which smart badges are located within the predefined boundary is based on the first and second wireless beacons (see page 9, paragraph 2 wherein a list of all beacons which inherently include first and second beacons are transmitted to the badge in other to detect which beacons are located in the room).

Regarding claim 29, Ljungh discloses the method of claim 28, wherein using the second wireless beacon comprises using the second wireless beacon to communicate with smart badges within the predefined boundary (page 17, paragraph 1 wherein beacons which inherently include first and second beacons communicate with the smart badges) and to communicate with smart badges outside the predefined boundary through one or more blocking objects defining the predefined boundary (see page 17, paragraph 6 wherein the signal are prone to travel through walls/outside boundary), and

using the first wireless beacon comprises using the first wireless beacon to communicate with smart badges within the predefined boundary (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge), wherein the first wireless beacon is blocked from communicating with smart badges outside the predefined boundary by the one or more blocking objects (see page 17, paragraph 5 wherein the frequency signal is limited to limited area).

Regarding claim 30, Ljungh discloses the method of claim 29, wherein using the first wireless beacon comprises using an infrared beacon (see page 3 section 2.2), and wherein using the second wireless beacon comprises using a radio frequency beacon (see page 17, section A.2).

Regarding claim 31, Ljungh discloses an article comprising a computer-usable medium containing program code that when executed cause a computer to:

store plural sub-sets of information (see page 13, section 4.1.1), each sub-set of information associated with one of plural clearance levels (see page 13, section 4.1.2, paragraph 1 wherein “access levels” is interpreted as “clearance levels” and the administrator assigns or determines who is able to view which information);

use at least a first wireless beacon to communicate with plural badges within a predefined region (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge), each of the plural badges associated with one of the plural clearance levels (see page 13, section 4.1.2, paragraph 1 wherein “access levels” is interpreted as “clearance levels” and the administrator assigns or determines who is able to view which information);

determine a lowest clearance level from among the clearance levels associated with the badges in the predefined region (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

provide access to one or more sub-sets of the information having one or more respective clearance levels no higher than the determined lowest clearance level (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 32, Ljungh discloses the article of claim 31, wherein providing access to the one or more sub-sets of the information comprises displaying the one or more sub-sets (see page 10, section 3.3.1 wherein the functionality displays information about person, rooms and objects stored in the database) of the information having the one or more respective clearance levels no higher than the determined lowest clearance level (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 33, Ljungh discloses the article of claim 31, wherein the program code when executed cause the computer to further:

use a second wireless beacon to communicate with the plural badges in the predefined region (page 17, paragraph 1 wherein beacons which inherently include first and second beacons communicate with the smart badges) and to communicate with one or more badges outside the predefined region (see page 17, paragraph 6 wherein the signal are prone to travel through walls/outside boundary),

wherein the first wireless beacon is able to communicate with the plural badges within the predefined region (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge) but is unable to communicate with the one or more badges outside the predefined region (see page 17, paragraph 5 wherein the frequency signal is limited to limited area); and determining the badges that are within the predefined region based on the first and second wireless beacons (see page 9, paragraph 2 wherein a list of all beacons which inherently include first and second beacons are transmitted to the badge in other to detect which beacons are located in the room).

Regarding claim 34, Ljungh discloses the article of claim 31, wherein the program code when executed cause the computer to further:

receive a parameter from each of the badges, the parameter indicating a confidence level that the respective badge has been worn continuously by a user (see page 15, section 4.2.1 paragraph 1 wherein the badge is authenticated to verify that the badge is in the possession of the owner).

Regarding claim 35, Ljungh discloses the article of claim 31, wherein the program code when executed cause the computer to further:

re-determine the lowest clearance level as badges enter or leave the predefined region (see page 5, paragraph 1 wherein person events is generated when moved from one room to another in the re-access the security access level).

Regarding claim 36, Ljungh discloses a system comprising:

Storage (see page 5, section 3.2.2) to store sub-sets of information associated with corresponding plural clearance levels (see page 13, section 4.1.2, paragraph 1 wherein “access levels” is interpreted as “clearance levels” and the administrator assigns or determines who is able to view which information);

a first wireless beacon to communicate wirelessly with badges within a predefined region (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge), each of the badges associated with one of the plural clearance levels (see page 13, section 4.1.2, paragraph 1 wherein “access levels” is interpreted as “clearance levels” and the administrator assigns or determines who is able to view which information);

a module to identify a lowest clearance level from among the clearance levels of the badges within the predefined region (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

software to provide access to one or more sub-sets of information in the storage having one or more clearance levels no higher than the identified lowest clearance level (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 37, Ljungh discloses the system of claim 36, further comprising:

a second wireless beacon to communicate wirelessly with badges within the predefined region (page 17, paragraph 1 wherein beacons which inherently include first and second beacons communicate with the smart badges) and at least one badge outside the predefined region (see page 17, paragraph 6 wherein the signal are prone to travel through walls/outside boundary),

wherein the first wireless beacon is unable to communicate with the at least one badge outside the predefined region (see page 17, paragraph 5 wherein the frequency signal is limited to limited area),

the module to detect the badges that are within the predefined region based on the first and second wireless beacons (see page 9, paragraph 2 wherein a list of all beacons which inherently include first and second beacons are transmitted to the badge in other to detect which beacons are located in the room).

Regarding claim 38, Ljungh discloses the system of claim 37, wherein the second wireless beacon comprises a radio frequency beacon (see page 17, section A.2), and the first wireless beacon comprises an infrared beacon (see page 3 section 2.2).

(10) Response to Argument

1. Claims 1 – 8, 11, 13 – 17, 21 – 28, 31 -33, 35, 36

(a) Other than reference to a guest badge and the fact that a guest badge has lower priority levels regarding access to certain areas, there is no teaching provided in § 4.2.8 of Ljungh of "identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary." This is a first point of error made by the Examiner (page 6, section 1, paragraph 3).

Examiner respectfully disagrees with the appellant. § 4.2.8 of Ljungh discusses both Guest badge and WIPS badge (smart badge). These badges are the same, perform the same functionality and could be assigned clearance levels. However, in § 4.2.8 of Ljungh, the lowest clearance level was identified for the Guest badge. Therefore, Examiner submits that the rejections for claim 1 as described in **(9) Grounds of Rejection above** which is applicable herewith and the response to appellant's argument provided herewith should be sustained.

(b) However, there is no teaching in § 4.2.1 of Ljungh of providing access to that sub-set of information having clearance level no higher than the lowest identified clearance level (page 7, paragraph 2).

Examiner respectfully disagrees with the appellant. In § 4.2.1, Ljungh discusses providing different security levels to different doors within a building. Different security levels are sub-set of the whole security system. On page 6, Ljungh discloses information about which badge a person is wearing and the IP address of his laptop. The badge is assumed to have static IP addresses that could be modified. Further on page 7, Ljungh discloses, “the database server has a method of finding out whether or not a particular user is allowed to see and update certain information in the database. These pages and section clearly suggests appellant’s claimed limitation “providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level”

In view of the response to argument (a) and (b) above and the rejection of claim 1 and it dependent claims, Examiner contends that claim 1 and its dependent claims are anticipated by Ljungh.

Independent claims 13, 21, 31, and 36 and their respective dependent claims are not allowable for similar responses as those regarding arguments of claim 1 above.

Therefore, Examiner submits that the rejections for claims 13, 21, and 36 as described in **(9) Grounds of Rejection above** which is applicable herewith and the response to appellant’s argument provided herewith should be sustained.

2. Claims 9, 18, 34.

Claims 9, 18, and 34 depend from independent claims 1, 13, and 31, respectively, and therefore are allowable for at least the same reasons as the corresponding base claims. Moreover, claim 9 recites defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers (page 9, section 2, paragraph 1).

Examiner respectfully disagrees with the appellant. Claims 9, 18, and 34 depend from independent claims 1, 13, and 31. As shown above claims 1, 13 and 31 are not allowable, therefore for the same reasons dependent claims 9, 18 and 24 are not allowable.

Moreover, Ljungh discloses whether each smart badge has been continuously worn by corresponding assigned smart badge wearers as shown on page 11, § 3.3.2 "The position of persons, peripherals and access points are drawn in real time on the map, If a person wearing a badge changes rooms, his or her position is updated on the map". Ljungh also discloses on page 15, § 4.2.1 that badges are authenticated to verify that the badges are in possession of the owner. These stated pages and sections fairly suggest appellant limitation "defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers" as in claim 9. Therefore, Examiner submits that the rejections for claims 9, 18 and 34 as described in **(9) Grounds of Rejection above** which is applicable herewith and the response to appellant's argument provided herewith should be sustained.

3. Claims 10 and 19.

Claims 10 and 19 depend from claims 1 and 13, and therefore are allowable for at least the same reasons as the corresponding base claims. Moreover, claim 10 recites assigning . . . However, the removal of data as performed in § 4.2.5 of Ljungh is not based on the expiration period (timeout noted on page 9 of Ljungh) having been exceeded. Therefore, claim 10 is not anticipated by Ljungh for this additional reason (page 10, section 3, paragraph 1).

Examiner respectfully disagrees with the appellant. Claims 10 and 19 depend from independent claims 1 and 13. As shown above claims 1 and 13 are not allowable, therefore for the same reasons dependent claims 10 and 19 are not allowable.

However, Ljungh discloses assigning an expiration period to each of the smart badges (see page 9, paragraph 1: ***"when a connection request from a badge is accepted….. .. or a timeout occurs" – inherently, expiration time has to be assigned before a timeout can occur)***; and de-authenticating and erasing all data stored on a smart badge whose expiration period has been exceeded (see page 14, section 4.1.5 paragraph 2: ***It is inherent as shown on this paragraph that access could be denied based on expiration of assigned time and the data on the badge that permits this access could be removed or erased based on this expiration time. The administrator has the authority to edit or remove data from the badge***).

These pages and sections fairly suggest appellant limitation "assigning an expiration period to each of the smart badges; and de-authenticating and erasing all data stored on a smart badge whose expiration period has been exceeded" as in claim 10 and similar limitation of claim 19. Therefore, Examiner submits that the rejections for claims 10 and 19 as described in **(9) Grounds of Rejection above** which is applicable herewith and the response to appellant's argument provided herewith should be sustained.

4. Claims 29, 30, 37, 38.

(a) Claims 29, 30, 37, and 38 depend from claims 1 and 36, respectively, and are therefore not anticipated by Ljungh for at least the same reasons as claim 1 and 36.

Examiner respectfully disagrees with the appellant. Claims 29, 30, 37, and 38 depend from independent claims 1 and 36. As shown above claims 1 and 36 are anticipated by Ljungh and are not allowable, therefore for the same reasons dependent claims 29, 30, 37 and 38 are not allowable.

(b) Therefore, it is clear that Ljungh does not disclose the use of both IR and RF beacons for the purpose of detecting which smart badges are located within the predefined boundary.

Claims 29, and its dependent claim, are thus further allowable for the above reasons.

Claim 37, and its dependent claim, are also further allowable for similar reasons as claim 29 (page 11, section 4, paragraph 3).

Examiner respectfully disagrees with the appellant. In § A.2, Ljungh discloses IR and RF that are placed as beacons inside a room and continuously transmit the room id information. Further on paragraph 1 of page 17 (§ A.1) Ljungh states “These beacons would emit a specific room id on a regular basis, which then could be detected by a smart device, a "badge", worn by the user. ………. The badge would then transmit the information received through an Ethernet connection via an attached wireless LAN card to a central server where the information would be processed and treated accordingly” The room id specifies the location of the smart badge.

Claims 29 and 37 and their respective dependent claims are not allowable for at least the responses to argument 4 (a) above. Therefore, Examiner submits that the rejections for claims 29, 30, 37, and 38 as described in **(9) Grounds of Rejection above** which is applicable herewith and the response to appellant's argument provided herewith should be sustained.

5. Claim 12, 20.

(a) Independent claim 12 is also not anticipated by Ljungh. More specifically, claim 12 recites identifying a lowest clearance level from among a plurality of clearance levels (assigned to the smart badges within the boundary), and providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary.

Examiner respectfully disagrees with the appellant. Ljungh discloses identifying a lowest clearance level assigned to the smart badges within the boundary (see page 16, section 4.2.8: the guest badge that is not different from ordinary badge is assigned lowest priority levels regarding access. Lowest priority level is interpreted as lowest clearance levels); and

providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (see page 7 section 3.2.3: Ljungh discloses ***"The database server also has methods for finding out whether or not a particular user is allowed to see and update certain information in the database) and also page 15, section 4.2.1 discloses***

wherein access is given in accordance different security levels. Different security levels are subset of the information or access);

Please also refer to response to argument 1(a) and 1(b) above that is applicable to claim 12 herewith.

(b) Moreover, claim 12 also recites recalculating the lowest clearance level in response to the change in smart badge visibility status. As discussed, the concept of a lowest clearance level is clearly not present in Ljungh. Therefore, the concept of recalculating the lowest clearance level would also not be taught by Ljungh (page 11, section 5)

Examiner respectfully disagrees with the appellant. Please refer to response to argument 1(a), 1(b) and 5(a) that discussed lowest clearance level. In addition, Ljungh discloses recalculating the lowest clearance level in response to the change in smart badge visibility status (see page 5, paragraph 1: ***"person events are also generated when the location of a person becomes unknown" and on page 9, paragraph 2, Ljungh also discloses "The server then makes a database lookup (persons are identified by the IP address of their badge) and updates the database if necessary" – Though not explicitly stated, updating the database implies changing access level/security level when the location of a person becomes unknown***).

Claims 12 and 20 are not allowable for at least the responses to argument 5(a) and 5(b) above. Therefore, Examiner submits that the rejections for claims 12 and 20 as described in **(9) Grounds of Rejection above** which is applicable herewith and the response to appellant's argument provided herewith should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

This examiner's answer contains a new ground of rejection set forth in section **(9)** above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be

treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

Respectfully submitted,

/Fred Ehichioya/

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

____

Conferees:

/John Breene/

Supervisory Patent Examiner, Art Unit 2162

/Tim T. Vo/

Supervisory Patent Examiner, Art Unit 2168

Tim Vo, Supervisory Patent Examiner, AU 2168